

Mobilní zranitelnosti

Ondřej Caletka

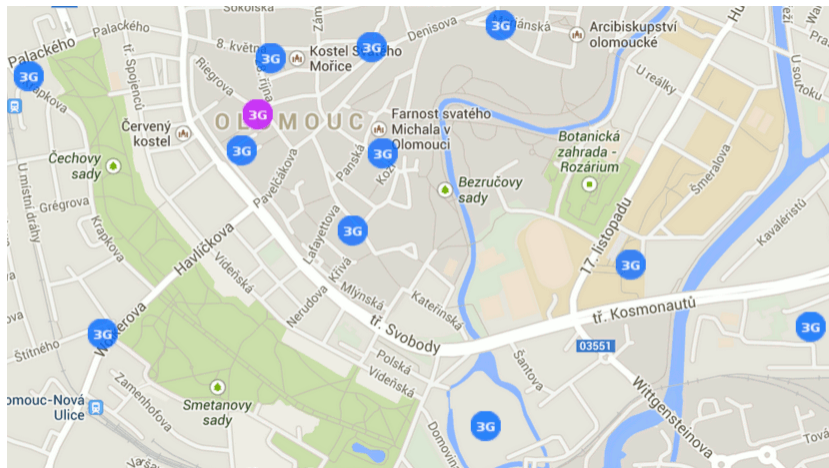


13. března 2014



Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

Geolokace mobilních zařízení

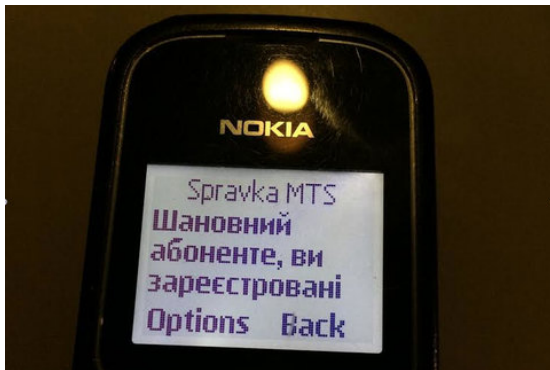


Zdroj: gsmweb.cz



Kijev, leden 2014

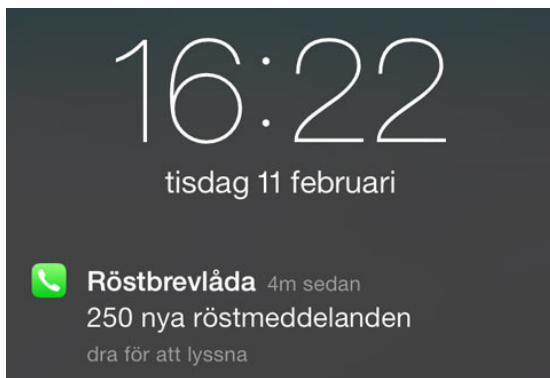
Vážený zákazníku, zaregistrovali jsme vás jako účastníka nepovolené demonstrace. Váš operátor.



Zdroj: nytimes.com

SMS zprávy

- původně jen servisní zprávy sítě
- nenesou jen text
- lidé jim mají tendenci důvěřovat



Zdroj: idg.se

CLIP (Identifikace volajícího)

- doplňková služba inteligentní sítě
- za validitu dat odpovídá originující operátor
- v rámci mezinárodního styku dobrovolné

Prozváněcí podvody

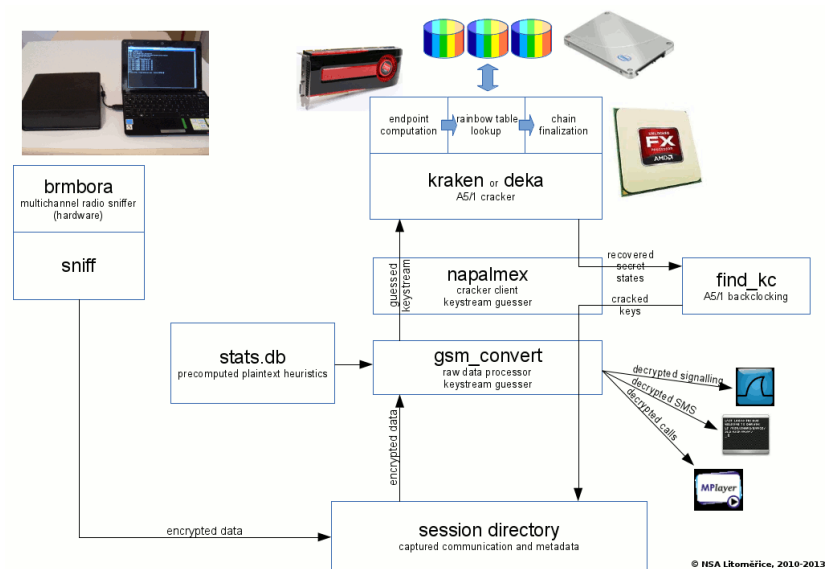
- Útočník provede krátký hovor z čísla například +2431230292
- Oběť volá zpět v domění, že jde o místní hovor
- Útočník (*spolu s místním operátorem*) profituje z astronomické ceny mezinárodního hovoru

příchozí hovor

Dobrý den, nabízím vám speciální tarif pouze pro vás,
Nejprve mi ale prosím sdělte heslo pro komunikaci s
operátorem...

- identifikaci volajícího lze poměrně snadno podvrhnout
- autentizace by měla být vzájemná
- autentizace by neměla umožnit převzetí identity protistrany (nesdělovat celé heslo, jen vybrané znaky)

Příliš děravé GSM



Zdroj: brmlab.cz

Příliš děravé GSM

- odposlech SMS zpráv k uživateli je realizovatelný v amatérských podmínkách
- ceny profesionálních zařízení stále klesají
- lze postavit falešnou BTS s vypnutým šifrováním
- moderní telefony nešifrovaný provoz nedokáží signalizovat
- částečným řešením je přechod na UMTS

Dvoufaktorová autorizace s mobilním telefonem

Problém roku ~2004

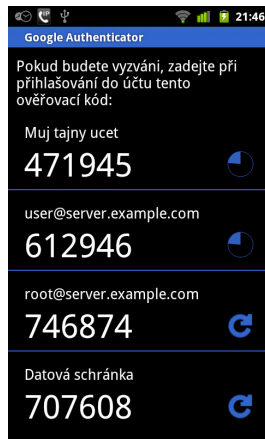
- lidé začali ve velké míře využívat e-banking
- jejich počítače byly prolezné malwarem
- ukradení jména a hesla (případně X.509 souboru z disku) bylo příliš lákavé

Přidání jednorázového SMS hesla

- kompromitace počítače nestačí
- kompromitace mobilního telefonu těžko realizovatelná
- obtížné propojení dat z kompromitovaných zařízení

Autentizační kalkulátor v mobilu

- Aplikace drží sdílené tajemství se serverem
- Z tajného klíče jsou podle aktuálního času odvozovány jednorázová hesla
- Standardizováno v RFC 6238, široká podpora v aplikacích:
 - Google
 - GitHub
 - MojID
 - Datové schránky



- lidé přestávají konzumovat obsah z PC
- banky se předhánějí, která nabídne lepší aplikaci pro smartphone
- lidé zadávají přihlašovací údaje *do téhož zařízení*, do kterého následně přichází ověřovací zpráva
- kompromitace mobilního zařízení nás vrací k problémům z roku 2004
ale útočník musí být schopen zneužití v reálném čase

Rizika mobilních aplikací

iPhone

- licence pro vývojáře
- přísné podmínky nabízení aplikací v App Store
- možnost nastavení oprávnění aplikací uživatelem

Android

- vývojář může být každý
- velmi otevřený Google Play Store
- oprávnění aplikací určuje vývojář



Česká pošta

eMan s.r.o

Aplikace má následující oprávnění:

Vaše poloha

přesná poloha (pomocí GPS a sítě)

Vaše zprávy

čtení textových zpráv (SMS nebo MMS)

příjem textových zpráv (SMS)

Síťová komunikace

úplný přístup k síti

Pozor na oprávnění

- odebrání oprávnění aplikaci uživatelem není na Androidu podporováno
- lze spoléhat jen na dobrou reputaci autora aplikace
- klíče k podepisování aplikace mohou být autorovi ukradeny

Root oprávnění

- aplikace s root oprávnění mohou *úplně všechno*
 - vstupovat do šifrovaných spojení
 - krást privátní klíče a hesla
 - maskovat se
- ani zařízení bez root nejsou v bezpečí

- nezkoušet všechny aplikace za každou cenu
- používat dvoufaktorovou autentizaci, kde je to možné, využívat hesla pro konkrétní zařízení
- omezit používání e-bankingu na mobilních zařízeních
- **nastavit zamykání obrazovky**

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<http://Ondrej.Caletka.cz>

